Case Study


# LiveIntent secures thousands of ephemeral devices daily with JupiterOne

# Meet Sean Cooper, VP of Information Security at LiveIntent

Sean Cooper joined LiveIntent three years ago to help build out their security program. As the company grew, and the security challenges evolved, Sean found that the security team needed better visibility into their environment and a better process for managing incident responses, audits, and day-to-day security operations.

The security team at LiveIntent discovered JupiterOne over a year ago and uses it daily to find data and insights about their environment that, according to Sean, "they would have a hard time finding otherwise."

**CHALLENGES**

## Securing thousands of ephemeral devices

LiveIntent has a highly dynamic workload within AWS. Every day, a couple thousand of AWS' large and expensive machines spin up for less than 12 hours, "do their thing," and then go away. All of them have to be governed, managed, and evaluated to ensure they're performing as intended and not introducing unexpected security risks.

Because of how AWS presents information across multiple accounts, and some other limited functionality of the native user interface in AWS, Sean and his team were having trouble finding the information they needed to manage all of their machines in AWS. They started looking for a product that could amalgamate all of their accounts into one place for better visibility and control.

### Project-based vs. Responsive security

LiveIntent, along with many information security teams, have two main buckets for security work: project-based and responsive.

**Project-based security** is centered around large projects like new security capabilities, yearly audits, and customer security information requests. These generally occur with some regularity and can be planned for.

**Responsive security**, or operational security, focuses more on the issues that crop up, seemingly unceasingly, throughout the work week. A large part of this responsive work is triaging and evaluating alerts.

Let's take a look at both types of work from the LiveIntent perspective.

> "We (InfoSec team) realize a lot of things about how our business runs that sometimes people don't tell us, or that we wouldn't have put together intuitively on our own. We've been very satisfied with JupiterOne and the service that comes with it.
>
> **Sean Cooper**
> *VP of InfoSec at LiveIntent*
>
> LiveIntent

SOLUTIONS

# Project-based security

Compiling information for audits, IRLs, and customer security requests with thousands of questions

## SOC2 Audit

Anyone who's been through a formal audit knows they can involve a lot of manual, time-consuming work gathering information and evidence and building out the proper frameworks and reporting.

LiveIntent recently completed their SOC2 audit. They were able to leverage the JupiterOne platform for evidence collection and correlation with the pre-built SOC2 framework. With all of their cyber asset information in one place, they were able to build queries, answer in-depth questions, and save those queries and answers as evidence.

Since dealing with information request lists (IRLs) can be a challenge, Sean and his team are working on creating roughly fifty IRLs that they can automate to avoid manually filtering through spreadsheets. Sean joked that the DevOps team is "salivating" at the thought of not having to do another audit and IRL manually.

LiveIntent is working with JupiterOne to move towards a fully automated SOC2 Audit experience in the future. Their goal for future audits is to progressively automate evidence collection and continuously perform control evaluation. They are building out queries and saving the information they will need to streamline the audit process for the next time around.

## Customer security requests

When customers or soon-to-be customers request information about platform security, LiveIntent needs to be able to provide accurate, honest answers. The questions in these requests can number in the thousands. JupiterOne helped LiveIntent streamline this process of gathering accurate, up-to-date information to answer the security questions, saving manual time and effort compiling the proper information.

> "JupiterOne has probably been the best tool I've touched. It's given us a lot of visibility into our environment. From an information security analyst perspective, it's become the go to for me and Adam whenever we're responding to incidents and day to day operations. We're able to glean a lot of information from it. It's been a great solution so far for our team.

**Ken**
*Information Security Analyst, LiveIntent*

LiveIntent

SOLUTIONS

# Responsive security

Improving Incident Response when native tools just don't do the trick

LiveIntent was having difficulty doing IR investigations in AWS because of a painfully slow and manual process, compounded by the inadequacy of the AWS UI. They needed a better solution to triage and respond to security events.

Incident Response (IR) includes triaging alerts and conducting investigative research to find what is connected to what, and who, etc. The goal of all of this digging is to qualify or disqualify an event as a security incident. If it is qualified as a potential security incident, the LiveIntent team needs to identify the root cause and find a solution.

> "Working with a tool like JupiterOne has been really eye opening for me. It lets us see what's out there and find and close gaps.
>
> **Adam**
> *Information Security Analyst, LiveIntent*
>
> LiveIntent

An up-to-date asset inventory is key to this process. Without a complete cyber asset inventory, and a simple way to access or query that inventory, it can be difficult to track down potential incidents. Since cyber assets encompass many types of resources, the LiveIntent team uses JupiterOne to collect and analyze data from every single "thing" in their technology stack and digital operations, including cloud service providers, HR systems, code repos, firewall rules, user endpoints, SaaS apps, IAM policies, security controls, vulnerability findings, and more. By aggregating all of this data, LiveIntent gets a holistic, centralized view of their cyber assets, including the relationships that they have with one another, all of which they can't get anywhere else.

The information security team at LiveIntent is alerted anytime something doesn't look right. Before finding JupiterOne, they were trying to evaluate their own reference materials and looking internally at AWS to find connection points and track down alerts. They were attempting to use the native AWS console and UI to find the root cause of security incidents.

Because of the volume of ephemeral devices they use (remember the thousands of machines that spin up and down every day and are active for less than 12 hours at a time?), navigating between different AWS accounts was quite cumbersome. According to Ken, "There is no one single view [in AWS] to see detailed information from all of your accounts. JupiterOne gathers all of this information together in one place so we can find what we need, rather than having 50 tabs open and trying to keep track of them."

The LiveIntent team needed a way to easily ask questions of their technology stack and cyber asset data. They couldn't query natively in AWS, and were impressed when they first saw the JupiterOne Query Language (J1QL). They have since become power users of J1QL, and often spend time digging into advanced queries with the JupiterOne customer success team, testing the limits of what asset data they can find with one single query.

RESULTS

## Uncovering more use cases for JupiterOne

We often say that creating a complete, accurate cyber asset inventory helps build the foundation for security operations. Once LiveIntent had full visibility into their environment and one central place to search their asset inventory, they were able to discover and add other functionality in JupiterOne, including compliance, policy mappings, and new queries for deeper incident response investigations. Some of the capabilities they have gained since using the JupiterOne platform include:

### Enforcing policies

Sean and his team found the policies module and quickly started the process of building out all policies in JupiterOne.

### Automating evidence collection

They are continuing to build new queries to automate evidence collection and future audit IRLs.

### Simplifying vendor management

LiveIntent is looking at streamlining their vendor management process in JupiterOne, replacing spreadsheets and Google forms for data collection.

### Bolstering AWS security

Sean, Ken, and Adam want to take advantage of JupiterOne's 40+ AWS service integrations, starting with native AWS security tools like AWS GuardDuty, AWS Security Hub, and AWS Config. There is potential for the team to replace other security tools in their tech stack, eliminating costs, and leveraging the combined functionality from AWS with the power and clarity they get from JupiterOne.

## When customer input meets our desire to never stop improving

JupiterOne is committed to continually improving our platform. We're constantly releasing new updates, adding integrations, and making more robust queries in a never ending quest to improve the user experience. We value input from our customers in this process. Our goal is to help them improve processes and workflows, as well as gather feedback on the platform to make it better.

The team at LiveIntent have been engaged with us from the start. Sean commented that "it's a bidirectional process. We meet on a regular basis with the JupiterOne Customer Success team to discuss queries, create new ones, and improve both the workflow and automation for LiveIntent, as well as bolster the JupiterOne Query Library and improve our overall product experience. If you're willing to work with us, we don't mind putting in the effort to get it working specifically for our processes. We saw the value right off the bat [from JupiterOne], and realized we could expand our usage as we grew."

## Conclusion

LiveIntent, like many other companies moving to the cloud, had a highly dynamic workload that was becoming unwieldy. They needed to amalgamate all of their cybersecurity asset and relationship data into one central repository. This complete cyber asset inventory became their foundation for incident response, day-to-day security operations, compliance automation, policy control, and a host of other security activities.

Whether you have a highly dynamic workload in AWS, GCP, Azure, or Alibaba Cloud, or simply can't find what you're looking for in the native consoles, JupiterOne can help. Contact JupiterOne today to schedule a demo and learn more.

## Major integrations include:

aws · bambooHR · GitHub · Google · jamf

Jira Software · KnowBe4 Human error. Conquered. · okta · slack · orca security

JupiterOne

JupiterOne is a cloud-native cyber asset attack surface management platform that enables security teams to solve persistent asset visibility and vulnerability challenges. Combine cyber asset data from all of your security tools into a single, unified view, and strengthen the foundation of your security program with JupiterOne.

Know what you have.
Focus on what matters.

Scan to Schedule a Demo ⟶

JupiterOne.com